Sarkar, Mohul (Student)

Palo Alto PA-410 Initial Configuration/SOHO Lab

Mohul Sarkar

**Purpose:**

Configuring Small Office/Home Office (SOHO) on a Palo Alto Networks PA-410 firewall involves setting up and optimizing the firewall for use in a small office or home office environment. This typically includes configuring basic network settings, such as IP addresses and subnet masks, as well as more advanced features such as security policies, firewall rules, and virtual private network (VPN) connections.

SOHO configuration also includes setting up the firewall to protect your internal network from external threats such as malware, intrusion and unauthorized access. This is done by creating security policies that define which traffic is allowed in and out of the network, and by configuring the firewall's threat prevention features to detect and block malicious traffic.

Additionally, SOHO configuration also includes setting up the firewall for VPN connectivity, which allows remote users to securely access the internal network and resources. This is done by configuring the firewall's VPN gateway and creating VPN policies that define which users are allowed to connect and what resources they have access to.

By properly configuring a PA-410 firewall in SOHO mode, users can ensure that their network is secure, reliable, and easy to manage.

**Background Information on Lab Concepts:**

I used SOHO previously in CCNP labs to configure security zones and in the past cybersecurity lab when I did the PA-220 SOHO. This configuration is very similar to that as you are creating the same security zones and the web interface for the PA-410 is like the Palo Alto web interface. I also previously have configured SOHO topologies from CCNA labs and am familiar with the commands needed to create a successful firewall to negate unauthorized access.

**Lab Summary:**

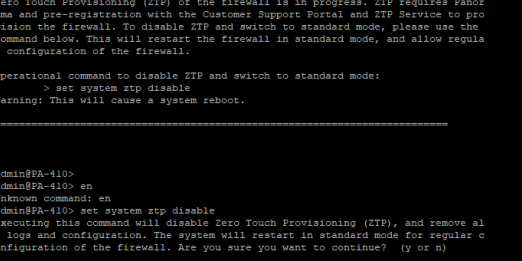
This lab setting up Small Office/Home Office (SOHO) on a Palo Alto Networks PA-410 firewall involves:

1. Configuring basic network settings such as IP addresses, subnet masks, and default gateway.
2. Creating security policies that define which traffic is allowed in and out of the network and configuring the firewall's threat prevention features to detect and block malicious traffic.
3. Setting up the firewall's VPN gateway and creating VPN policies that allow remote users to securely access the internal network and resources.
4. Configuring advanced features such as firewall rules, security zones, and virtual routers.
5. Testing and verifying the configuration to ensure that the network is secure, reliable, and easy to manage.
6. Troubleshoot and fine tuning the configuration to optimize the performance.

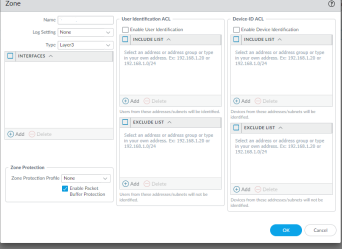
Overall, the lab would provide hands-on experience in configuring a PA-410 firewall for use in a small office or home office environment, including setting up basic network settings, creating security policies, and configuring advanced features such as VPN and firewall rules.

**Lab Commands:**

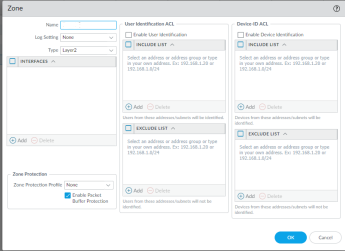
1. Go into web browser and enter https://192.168.1.1, go into advanced options and ignore security threat to enter PA-410 web interface
2. Enter PuTTY and enter “set system ztp disable” to be able to enter the web interface after the ZTP mode selection screen



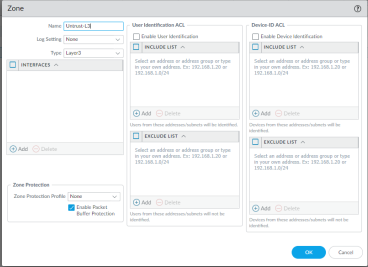
1. Enter Network-> Zones -> Add and create a Layer 3 “Trust-L3” zone



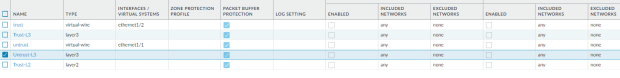
1. Create another Zones -> Add and make a Layer 2 “Trust-L2”



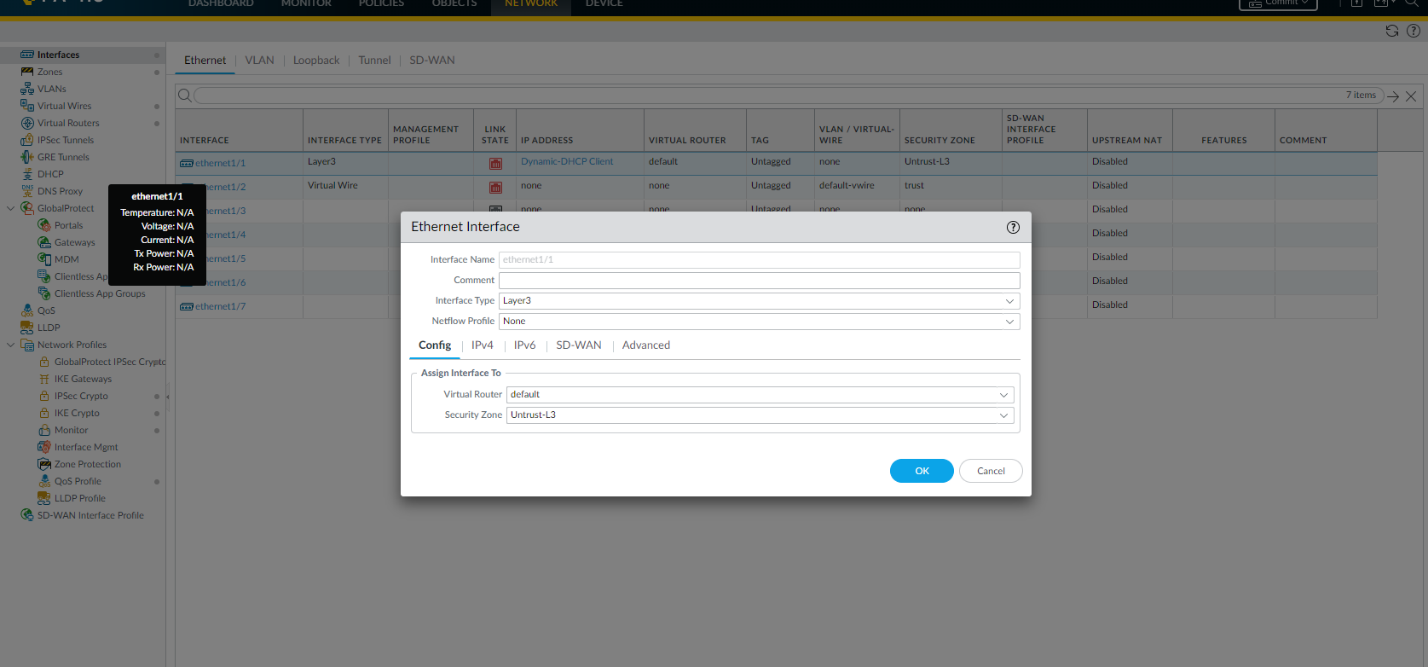
1. Once again, create another zone and name “Untrust-L3” and set it to Layer 3



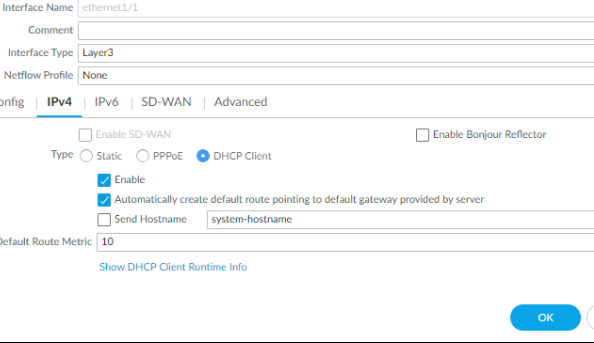
1. After configuring all zones, you should be able to see them listed with their zones and their layer.



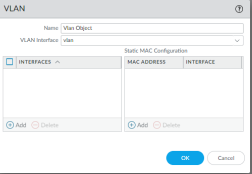
1. Next to configure the ethernet interfaces go to Network -> Interfaces -> Add and add a new interface on Layer 3 with the Untrust-L3 security zone.



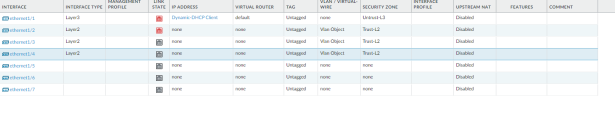
Next in the same screen, enter IPv4 and set the router to DHCP and automate the default route



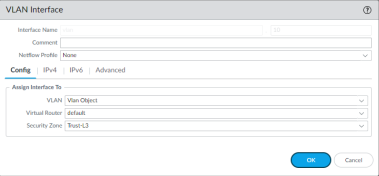
1. Next to create the VLANs enter Network -> VLAN -> Add a VLAN Object

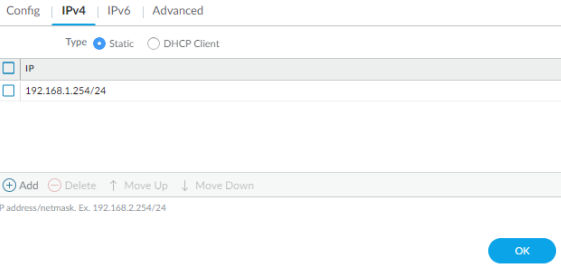


1. Then assign ethernets 1-2, 1-3 and 1-4 to this VLAN object and make sure the link state of ethernet 1-1 is up and running with DHCP

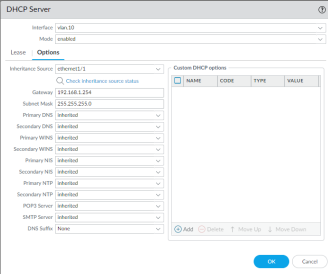


1. Create a new VLAN and configure it with an ip address in the IPv4 tab of the same window

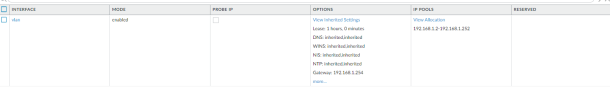




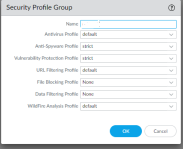
1. Next to create a DHCP Sever, enter Network -> DHCP -> Options and name and set the ip address to what you gave the previous VLAN



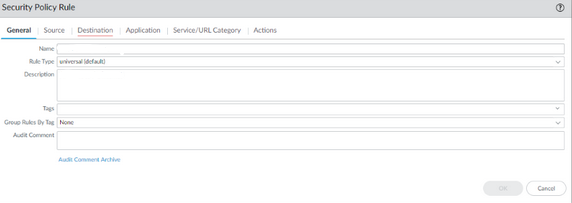
1. Verify the settings are applied to the DHCP Server by looking at the web interface containing the changed settings



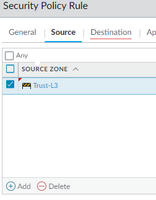
1. Next enter Network -> Security Profile Groups and create a new default Security Profile group

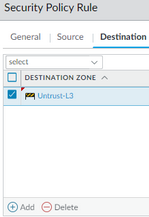


1. Next after creating a Security Profile Group, enter Policies -> Security and set a new Security Policy Rule for all outgoing security traffic

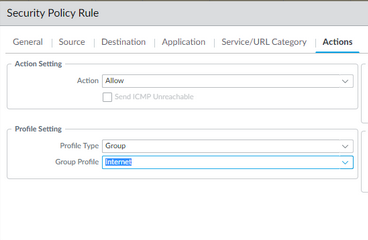


1. Next, apply new settings to both Untrust-L3 and Trust-L3

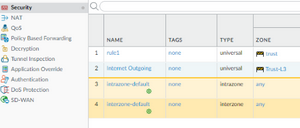




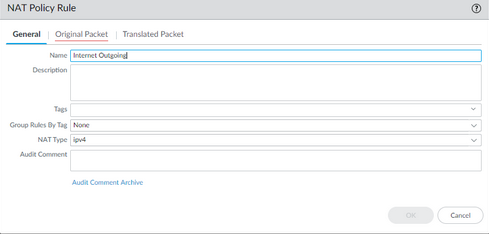
1. After creating these Security Policy Rules enter the “Actions” tab and name the Group Profile “Internet”



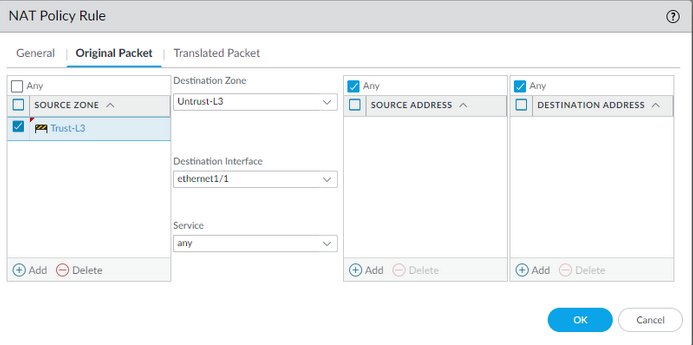
1. When in Policy -> Security tab you should now be able to see an overview of all of the policies you have just applied



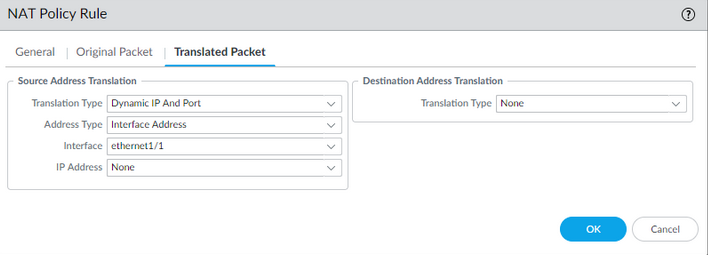
1. Next, select Policies -> NAT -> Add and create a new NAT Policy rule for outgoing internet traffic



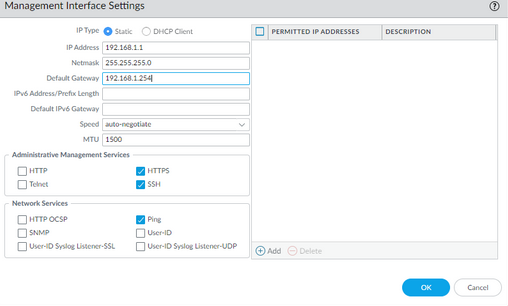
1. Within the same window, navigate to the “Original Packet” tab and select Trust-L3 for the Source Zone, ethernet1/1 for the destination interface and Untrust-L3 for the Destination Zone



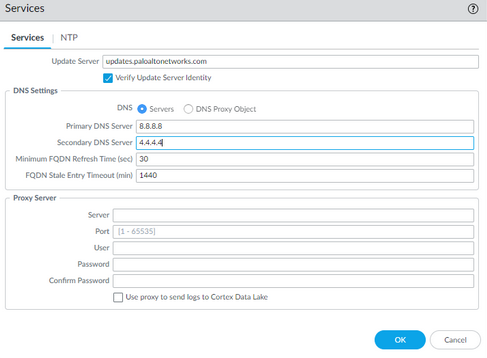
1. Once again on the same window, select the next tab labeled “Translate Packet” and set the interface to ethernet1/1 and Dynamic IP and Port



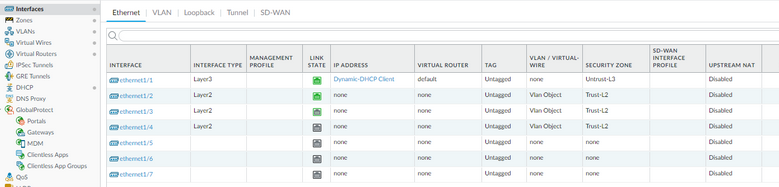
1. Enter Device -> Setup -> Management Interface Settings and set the default gateway to “192.168.1.254” and the ip address to static “192.168.1.1”



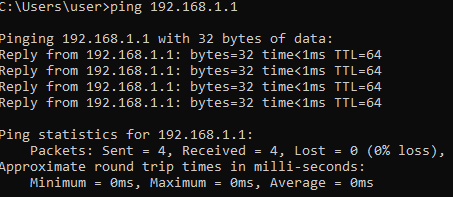
1. Within the same window, enter “Services” and enter the window and apply a default DNS address



1. After applying Services settings, enter Network -> Interface and look at the overview of all the routers and connectivity



1. Verify connectivity by pinging through firewall to computer and debug until successful pings are sent



1. After debugging and receiving successful pings from assigned ip address SOHO has effectively been configured
2. LAB COMPLETE

**Problems:**

As I set up the routing protocols, I incorrectly set an Ip address making the firewall not function properly and resulted in an insufficient network. After solving this problem, I was able to ping from the router and there were effective SOHO settings applied, optimizing the flow of traffic through the firewall. Another problem I ran into was I also did not apply the settings on the access control list. This change made it possible for unauthorized users to gain access to sensitive data and malicious traffic could enter the network due to incorrect filtering.

**Conclusion:**

This lab gave a more in depth understanding of SOHO configurations and how they can span from different Palo Alto router. As this lab was very similar to the previous Palo Alto SOHO lab, the configuration seemed familiar and the problem for the lab were minimal as most of the bugs in the previous lab were learned from when applying the same knowledge in this lab. Learning simple and applicable networking topologies such as SOHO can be helpful in the real world if you are planning on setting up a home office network and want to create some sort of network traffic security. The inexpensiveness of SOHO along with the effective security makes it a very important lab concept to know for real life application and to build off of as a baseline for labs that use SOHO topologies.